ACTUALIZACIÓN NORMA ISO/IEC 27001:2005 PARA LA VERSIÓN 2013 EN CARACOL TELEVISIÓN

ADAN RICARDO CASTILLO PLATA

FUNDACÍON UNIVERSITARIA LOS LIBERTADORES

FACULTAD DE INGENIERÍA

PROGRAMA SISTEMAS

BOGOTÁ

2015

ACTUALIZACIÓN NORMA ISO/IEC 27001:2005 PARA LA VERSIÓN 2013 EN CARACOL TELEVISIÓN

ADAN RICARDO CASTILLO PLATA

Trabajo de grado para optar al título de Ingeniero de Sistemas

DIRECTOR
AUGUSTO JOSE ANGEL MORENO

FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES

FACULTAD DE INGENIERÍA

PROGRAMA SISTEMAS

BOGOTÁ

2015

Tabla de contenido

Tabla de figuras

INTRODUCCIÓN

En la actualidad con el avance tecnológico de forma exponencial y con la vinculación de estas innovaciones a los distintos aspectos de la vida cotidiana permite el intercambio de datos e información para facilitar la productividad y la comunicación entre las personas, conllevando al desarrollo personal de igual forma que el empresarial. El manejo de la información en la vida cotidiana sea cual sea su uso tiene un gran valor, normalmente se cree que la información manejada si no son contraseñas, datos financieros o cuentas electrónicas no tiene valor alguno pero eso depende de cómo se use, el más pequeño dato puede revelar una gran cantidad de información.

En consecuencia con las nuevas tecnologías van apareciendo nuevos riegos que busca lo más valioso de las personas y de las empresas; la información. El cual es un activo que todas las personas manejan y que debería ser protegido respectivamente sin importar su clasificación o valor, pero en la realidad no se toma las mínimas medidas para resguardar o preservar.

Para evitar que la información que se maneja dentro de Caracol Televisión sea expuesta a terceros o personas malintencionadas, se ha iniciado la actualización de la norma ISO/IEC 27001:2005 a la versión del 2013 con respecto a los nuevos controles de la ISO/IEC 27002 para proteger los recursos de información que son importantes, actualizando las medidas para salvaguardar la información y buscando de esta manera brindar una protección adecuada para las nuevas tecnologías.

1. JUSTIFICACIÓN

Con el presente proyecto se procura apoyar con el proceso de actualización de la norma ISO/IEC 27001 con respecto a los nuevos controles agregados en la versión del año 2013, los cuales buscan asegurar la información conforme a las nuevas tendencias tecnológicas que se presentan y traen consigo las nuevas vulnerabilidades a los sistemas actuales, y por consiguiente generan riesgos contra los recursos informáticos, estableciendo en consecuencia nuevas medidas, políticas y controles capaces de mitigar los incidentes producidos por la nueva tecnología.

La actualización de la norma ISO se debe a que Caracol Televisión se encuentra implementando un nuevo gestor empresarial conocido como SAP el cual mejora el rendimiento y producción que genera el sistema anterior, pero dicho cambiado traen consigo nuevas fallas y vulnerabilidades en los sistemas. De igual forma para se diseña un sistema de gestión de seguridad informática para reforzar las políticas y lograr mitigar vulnerabilidades.

Sí las vulnerabilidades no son investigadas puede ocurrir el incidente que a finales del 2014 se presentó, uno de los ataque informáticos más representativos de la historia a una empresa multinacional reconocida, como resultado se produjo una gran filtración de archivos interna de la organización entre los cuales se encontraron: estados financieros, información confidencial de todos los empleados, información confidencial que trataba las directivas de la organización, nuevas y futuras inversiones, entre otros. Concluyendo en una pérdida de más de $500 millones de dólares sin contar con los futuros problemas que pueden acarrear por culpa del incidente de seguridad y la pérdida de confianza en la marca.

Este incidente se presentó por fallas en las políticas, mal manejo de la gestión de documentación y activos, controles de seguridad poco apropiados y demás fallas que por motivos de seguridad para evitar una reincidencia al incidente no se han revelado. Debido al riesgo de tener políticas desactualizadas y controles establecidos básicos en el momento que exista un incidente informático con grandes magnitudes y con daños considerablemente grandes, Caracol Televisión no está preparado para ese tipo de eventos.

2. OBJETIVOS

2.1 GENERAL

Actualizar e implementar los nuevos controles establecidos dentro de la norma ISO/IEC 27001:2013 dentro de las instalaciones de Caracol Televisión.

2.2 ESPECÍFICOS

- Identificar los controles para actualizar teniendo en cuenta las nuevas tecnologías a implementar.
- Actualizar las distintas normas y guías de seguridad informática implementadas hasta el 2013.
- Realizar las modificaciones correspondientes a la normatividad interna.
- Validar las actividades implementadas en los controles de la norma ISO, en la versión del año 2005.
- Fortalecer los conocimientos a nivel organizacional sobre seguridad de la información.
- Comprometer al personal de Caracol Televisión para la implementación de las nuevas técnicas en la seguridad de la información.

3. MARCO TEÓRICO

3.1 NORMA ISO/IEC 27001

La ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.[1]

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

ISO 27001 se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento.

La norma ISO 27001 también es un elemento de la seguridad relacionado con el alojamiento en los datos en la nube. Esta norma, publicada por la ISO (International Organization for Standarization), describe las exigencias para la implementación de un Sistema de Gestión de la Seguridad de la información.

Este SGSI debe definir las medidas de seguridad que se deberán aplicar en el SI para asegurar la protección de los bienes de una empresa. Con el objetivo de garantizar una mejora continua de la seguridad del SI, la norma ISO 27001 se basa en el modelo de calidad PDCA (Plan Do Check Act).[2]

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

[1] 27001Academy. Disponible en: <http://www.iso27001standard.com/es/que-es-iso-27001/>

[2] ACISSI, et al., Seguridad informática - Ethical Hacking: Conocer el ataque para una mejor defensa. 2ª edición, p. 368.

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

Figura 1. Estructura de ISO 27001

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software pero son utilizados de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.

Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, personas, bienes, entre otros, ISO 27001 ha detallado cómo amalgamar todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI).

Por eso, la gestión de la seguridad de la información no se acota solamente a la seguridad de TI (por ejemplo, cortafuegos, anti-virus, entre otros), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, entre otros.

Hay 4 ventajas comerciales esenciales que una empresa puede obtener con la implementación de esta norma para la seguridad de la información:

Cumplir con los requerimientos legales – cada vez hay más y más leyes, normativas y requerimientos contractuales relacionados con la seguridad de la información. La buena noticia es que la mayoría de ellos se pueden resolver

implementando ISO 27001 ya que esta norma le proporciona una metodología perfecta para cumplir con todos ellos.

Obtener una ventaja comercial – si su empresa obtiene la certificación y sus competidores no, es posible que usted obtenga una ventaja sobre ellos ante los ojos de los clientes a los que les interesa mantener en forma segura su información.

Menores costos – la filosofía principal de ISO 27001 es evitar que se produzcan incidentes de seguridad, y cada incidente, ya sea grande o pequeño, cuesta dinero; por lo tanto, evitándolos su empresa va a ahorrar mucho dinero. Y lo mejor de todo es que la inversión en ISO 27001 es mucho menor que el ahorro que obtendrá.

Una mejor organización – en general, las empresas de rápido crecimiento no tienen tiempo para hacer una pausa y definir sus procesos y procedimientos; como consecuencia, muchas veces los empleados no saben qué hay que hacer, cuándo y quién debe hacerlo. La implementación de ISO 27001 ayuda a resolver este tipo de situaciones ya que alienta a las empresas a escribir sus principales procesos (incluso los que no están relacionados con la seguridad), lo que les permite reducir el tiempo perdido de sus empleados.

La versión 2013 establece cambios en el contenido de la norma asimismo como en la estructura, lo que se reflejará en otros documentos que forman parte de la familia ISO-27000.

La ISO/IEC 27001:2013 fue creada haciendo referencia al anexo SL de la norma ISO/IEC del “Suplemento Consolidado de las Directivas ISO/IEC” publicado en la “Guía ISO: 83”, la cual indica los lineamientos a seguir para el desarrollo documental de un sistema de gestión con una estructura para todos los documentos relacionados con el sistema de gestión. De esta manera, la estructura de la nueva versión de la ISO/IEC 27001:2013 con respecto a la 2005 queda:

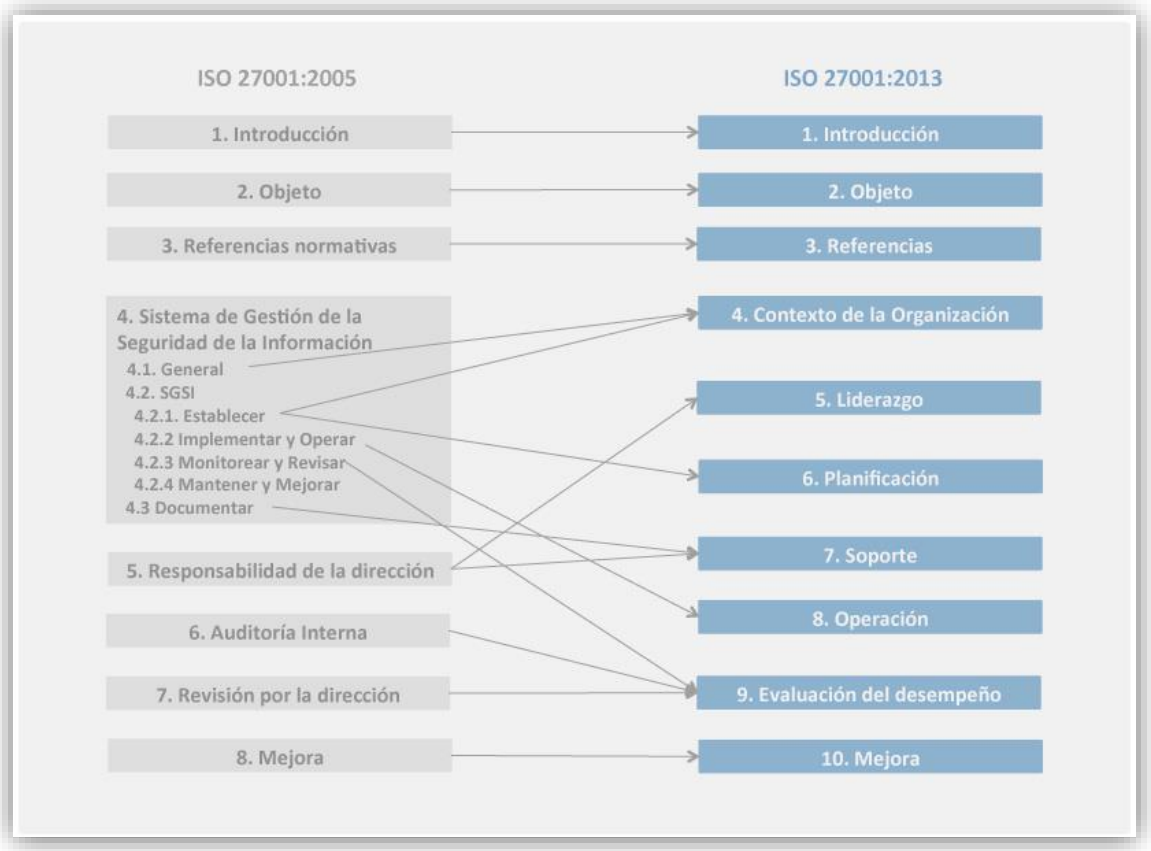

Figura 2. Diferencia estructural ISO 27001: 2005 y 2013[3]

A nivel de controles (Anexo A) se puede comentar que aunque aumentó el número de dominios de seguridad de 11 a 14, esto se debió fundamentalmente a una reestructura del estándar pues por ejemplo el dominio A.10 Administración de Comunicaciones y Operaciones de la versión 2005 ahora se separó en dos dominios, así como también se creó un dominio específico para Criptografía y otro para la Relación con proveedores, derivado de dicha reestructura el número de controles disminuyó pasando de 133 a 113, a continuación se muestra el listado comparativo de los nuevos dominios de seguridad de la información.

[3] PMG-SSI. Disponible en: <http://www.pmg-ssi.com/2014/11/iso-270012015-un-cambio-en-la-integracion-de-los-sistemas-de-gestion/>

Anexo A ISO 27001:2005	Anexo A ISO 27001:2013
A.5 Política de Seguridad	A.5 Políticas de Seguridad
A.6 Organización de seguridad de la información	A.6 Organización de la seguridad de la información
A.8 Seguridad en recursos humanos	A.7 Seguridad en recursos humanos
A.7 Administración de activos	A.8 Administración de activos
A.11 Control de acceso	A.9 Control de acceso
	A.10 Criptografía
A.9 Seguridad física y ambiental	A.11 Seguridad física y ambiental
A.10 Administración de comunicaciones y operaciones	A.12 Seguridad en operaciones
	A.13 Seguridad en comunicaciones
A.12 Adquisición, desarrollo y mantenimiento de sistemas	A.14 Adquisición, desarrollo y mantenimiento de sistemas
	A.15 Relación con proveedores
A.13 Administración de incidentes de seguridad de la información	A.16 Administración de incidentes de seguridad de la información
A.14 Administración de continuidad del negocio	A.17 Aspectos de seguridad de la información en la administración de continuidad del negocio

Figura 3. Cambios de controles de seguridad de información en el anexo A[4]

3.2 NORMA ISO/IEC 27002

La norma ISO 27002 fue publicada originalmente como un cambio de nombre de la norma ISO 17799 vigente, un código de prácticas para la seguridad de la información. Básicamente describe cientos de posibles controles y mecanismos de control, que pueden ser implementadas, en teoría, con sujeción a la orientación proporcionada en la norma ISO 27001.

La base de la norma fue originalmente un documento publicado por el gobierno del Reino Unido, que se convirtió en un estándar "adecuado" en 1995, cuando fue re-publicado por BSI como BS7799. En 2000 se volvió a re-publicado, esta vez por la ISO, como ISO 17799. Una nueva versión de este apareció en 2005, junto con una nueva publicación, la norma ISO 27001. Estos dos documentos están destinados a ser utilizados en conjunto, con uno complementando la otra.

[4] QualityTrends. Disponible en: <http://qualitytrends.squalitas.com/index.php/item/186-principales-cambios-de-la-nueva-version-de-iso-27001>

En 2013 se publicó la versión actual ISO 27002: 2013 contiene 114 controles, en comparación con el 133 documentado dentro de la versión 2005. Sin embargo, para granularidad adicional, éstos se presentan en catorce secciones, en lugar de los once inicial.

Por último, cabe señalar que en los últimos años se han desarrollado una serie de versiones específicas de la industria de la norma ISO 27002, o se encuentran en fase de desarrollo, (por ejemplo: sector de la salud, manufactura, etc.)[5].

3.3 SEGURIDAD INFORMÁTICA

La seguridad informática consiste en asegurar en que los recursos del sistema de información de una organización se utilicen de la manera que se decidió y que el acceso a la información allí contenida así como su modificación solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

3.3.1 Fiabilidad, confidencialidad, integridad y disponibilidad

Si bien es cierto que todos los componentes de un sistema informático están expuestos a un ataque, son los datos y la información los sujetos principales de protección de las técnicas de seguridad. La seguridad informática se dedica principalmente a proteger la confidencialidad, la integridad y la disponibilidad de la información, por tanto, actualmente se considera que la seguridad de los datos y la información comprenden 3 aspectos fundamentales:

- Confidencialidad
- Integridad (seguridad de la información)
- Disponibilidad

Hay que tener en cuenta que tanto las amenazas como los mecanismos para contrarrestarla suelen afectar a estas 3 características de forma conjunta por tanto un fallo del sistema que haga que la información no sea accesible puede llevar consigo una pérdida de integridad. Generalmente tiene que existir los 3 aspectos descritos para que haya seguridad. Dependiendo del entorno en el que trabaje un sistema, a sus responsables les interesará dar prioridad a un cierto aspecto de la seguridad. Junto a estos 3 conceptos fundamentales se suele estudiar

[5] The ISO 27000 Directory. Disponible en: <http://www.27000.org/iso-27002.htm>

conjuntamente la autenticación y el no repudio. Suele referirse al grupo de estas características como CIDAN, nombre sacado de la inicial de cada característica.

Los diferentes servicios de seguridad dependen unos de otros jerárquicamente, así si no existe el primero no puede aplicarse el siguiente.
Disponibilidad: Se trata de la capacidad de un servicio, de unos datos o de un sistema a ser accesible y utilizable por los usuarios o procesos autorizados cuando lo requieran. También se refiere a la capacidad de que la información pueda ser recuperada en el momento que se necesite.

Confidencialidad: Se trata de la cualidad que debe poseer un documento o archivo para que éste solo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado.
Un ejemplo de control de la confidencialidad sería el uso cifrado de clave simétrica en el intercambio de mensajes.

Integridad: Es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original.

Alta disponibilidad: son sistemas que están disponibles las 24 horas al día, 7 días a la semana, 365 días al año.

La disponibilidad se presenta en niveles:

- Base: Se produce paradas previstas e imprevistas.
- Alta: Incluyen tecnologías para disminuir el número y la duración de interrupciones imprevistas aunque siempre existe alguna interrupción imprevista.
- Operaciones continuas: Utilizan tecnologías para asegurar que no hay interrupciones planificadas
- Sistemas de disponibilidad continua: Se incluyen tecnologías para asegurarse que no habrá paradas imprevistas ni previstas.
- Sistemas de tolerancia al desastre: requieren de sistemas alejados entre sí para asumir el control en una interrupción provocada por un desastre.

Autenticación: Es la situación en la cual se puede verificar que un documento ha sido elaborado o pertenece a quien el documento dice. La autenticación de los sistemas informáticos se realiza habitualmente mediante nombre y contraseña.

No repudio: El no repudio o irrenunciabilidad es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación.
Existen 2 posibilidades:

- No repudio en origen: el emisor no puede negar el envío porque el destinatario tiene pruebas del mismo el receptor recibe una prueba infalsificable del envío.
- No repudio de destino: el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción.

Si la autenticidad prueba quien es el autor y cuál es su destinatario, el no repudio prueba que el autor envió la comunicación (en origen) y que el destinatario la recibió (en destino).

3.3.2 Elementos vulnerables en un sistema informático: hardware, software y datos.

Seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia conviene aclarar que no siendo posible la certeza absoluta el elemento de riesgo está siempre presente independientemente de las medidas que tomemos por lo que debemos hablar de niveles de seguridad, la seguridad absoluta no es posible y en adelante entenderemos que la seguridad informática es un conjunto de técnicas encaminadas a obtener niveles altos de seguridad, la seguridad es un problema integral, los problemas de seguridad informática no pueden ser tratados aisladamente ya que la seguridad de todo el sistema es igual a su punto más débil. El uso de sofisticados algoritmos y métodos es inútil si no garantizamos la confidencialidad de las estaciones de trabajo, por otra parte, existe algo que los hackers llaman ingeniería asociada que consiste simplemente en conseguir mediante un engaño que los usuarios autorizados revelen sus passwords, por lo tanto la educación de los usuarios es fundamental para que la tecnología de seguridad pueda funcionar.

Los 3 elementos principales a proteger en cualquier sistema informático son el software, el hardware y los datos. Por hardware se entiende por el conjunto de todos los elementos físicos de un sistema informático como CPU, terminales, cableados, medios de almacenamiento secundarios, tarjeta de red, etc... Por software se entiende por el conjunto de programas lógicos que hace funcionar el hardware tanto sistemas operativos como aplicaciones y finalmente por datos se entiende el conjunto de información lógica que maneja el software y el hardware, como por ejemplo paquetes que circulan por un cable de red, o una entrada a una base de datos.

Habitualmente los datos constituyen los 3 principales elementos a escoger ya que es el más amenazado y seguramente el más difícil de recuperar. También tenemos que ser conscientes de que las medidas de seguridad que deberán establecerse comprenden el hardware el sistema operativo, las comunicaciones, medidas de seguridad física, controles organizativos y legales.

3.3.3 Las amenazas.

Las amenazas de un sistema informático pueden provenir desde un hacker remoto que entra en nuestro sistema desde un troyano, pasando por un programa descargando de forma gratuita que nos ayuda a gestionar nuestras fotos pero que supone una puerta trasera a nuestro sistema permitiendo la entrada a espías hasta la entrada no deseada al sistema mediante una contraseña de bajo nivel de seguridad; se pueden clasificar por tanto en amenazas provocadas por personas, lógicas y físicas. A continuación se presenta a una relación de los elementos que potencialmente pueden amenazar a nuestro sistema. La primera son las personas, la mayoría de los ataques a nuestro sistema van a provenir de forma intencionada o inintencionada de personas y pueden causarnos enormes pérdidas. Aquí se describen brevemente los diferentes tipos de personas que pueden constituir un riesgo para nuestros sistemas:

3.3.3.1 Personas

- Personal (se pasa por alto el hecho de la persona de la organización incluso a la persona ajeno, a la estructura informática, puede comprometer la seguridad de los equipos).
- Ex-empleados (generalmente se trata de personas descontentas con la organización que pueden aprovechar debilidades de un sistema del que conocen perfectamente, pueden insertar troyanos, bombas lógicas, virus o simplemente conectarse al sistema como si aún trabajaran en la organización).
- Curiosos (son los atacantes juntos con los crackers los que más se dan en un sistema).
- Hackers (una persona que intenta tener acceso no autorizado a los recursos de la red con intención maliciosa aunque no siempre tiende a ser esa su finalidad).
- Crackers (es un término más preciso para describir una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa).
- Intrusos remunerados (se trata de personas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema que son pagados por una tercera parte generalmente para robar secretos o simplemente para dañar la imagen de la organización).

3.3.3.2 Amenazas lógicas

- Software incorrecto(a los errores de programación se les llama Bugs y a los programas para aprovechar uno de estos fallos se les llama Exploits.)
- Herramientas de seguridad (cualquier herramienta de seguridad representa un arma de doble filo de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o la subred completa un intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos, herramientas como NESUS, SAINT o SATAN pasa de ser útiles a peligrosas cuando la utilizan Crackers.)
- Puertas traseras (durante el desarrollo de aplicaciones grandes o sistemas operativos es habitual que entre los programadores insertar atajos en los sistemas habituales de autenticación del programa o núcleo de sistema que se está diseñando.) Son parte de código de ciertos programas que permanecen sin hacer ninguna función hasta que son activadas en ese punto la función que realizan no es la original del programa si no una acción perjudicial.)
- Canales cubiertos (son canales de comunicación que permiten a un proceso trasferir información de forma que viole la política de seguridad del sistema.)
- Virus (un virus es una secuencia de código que se inserta en un fichero ejecutable denominado huésped de forma que cuando el archivo se ejecuta el virus también lo hace insertándose a sí mismo en otros programas.)
- Gusanos(es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes en ocasiones portando virus o aprovechando bugs de los sistemas a los que se conecta para dañarlos a ser difíciles de programar su número no es muy elevado pero el daño que causa es muy grave.)
- Caballos de troya (son instrucciones escondidas en un programa de forma que este parezca realizar las tareas que un usuario espera de él pero que realmente ejecuta funciones ocultas).
- Programas conejo o bacterias (bajo este nombre se conoce a este programa que no hace nada útil si no que simplemente se delimitan a reproducirse hasta que el número de copias acaba con los recursos del sistema produciendo una negación del servicio.

3.3.3.3 Amenazas Físicas: Robos, sabotajes, destrucción de sistemas. Suministro eléctrico. Condiciones atmosféricas. Catástrofes naturales

Formas de protección de nuestro sistema: Para proteger nuestros sistemas se debe realizar una análisis de las amenazas potenciales, las pérdidas que podrían generar y la probabilidad de ocurrencia, a partir de este análisis se debe diseñar una política de seguridad que defina responsabilidades y reglas a seguir para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan, a esto se le llama mecanismo de seguridad, son la herramienta básica para

garantizar la protección de los sistemas o la red. Estos mecanismos se pueden clasificar en activas o pasivas.

- Activas: evitan daños en los sistemas informáticos mediante empleo de contraseñas adecuadas en el acceso a sistemas y aplicaciones, encriptación de los datos en las comunicaciones, filtrado de conexiones en redes y el uso de software específico en seguridad informática.
- Pasiva: minimizan el impacto y los efectos causados por accidentes mediante uso de hardware adecuado, protección física, eléctrica y ambiental, realización de copias de seguridad.[6]

3.4 DRP

Un plan de recuperación de desastre (DRP) –a veces conocido como un plan de continuidad de negocios (BCP) o plan de contingencia de procesos de negocio (BPCP)- describe cómo enfrenta una organización posibles desastres. Así como un desastre es un evento que imposibilita la continuación de las funciones normales, un plan de recuperación de desastre se compone de las precauciones tomadas para que los efectos de un desastre se reduzcan al mínimo y la organización sea capaz de mantener o reanudar rápidamente funciones de misión crítica. Por lo general, la planificación de recuperación de desastre implica un análisis de los procesos de negocio y las necesidades de continuidad; también puede incluir un enfoque significativo en la prevención de desastres.

La recuperación de desastres se está convirtiendo en un aspecto cada vez más importante de la informática empresarial. Como los dispositivos, sistemas y redes se vuelven cada vez más complejos, simplemente hay más cosas que pueden salir mal. Como consecuencia de ello, los planes de recuperación se han vuelto más complejos. Según Jon William Toigo (autor de la Planificación de Recuperación de Desastres). Por ejemplo, hace quince o veinte años, si había una amenaza de incendio para los sistemas, un plan de recuperación de desastres podría consistir en apagar la computadora central y otros equipos antes de que el sistema de rociadores se encendiera, desmontar componentes, y posteriormente secar las placas de circuitos en el estacionamiento con un secador de pelo. Sin embargo, los actuales sistemas empresariales tienden a ser demasiado grandes y complicados para estos métodos sencillos y prácticos, y la interrupción del servicio o la pérdida de datos pueden tener consecuencias financieras graves, ya sea directamente o a través de la pérdida de confianza del cliente.

[6] TANGIENT LLC. Wikispaces. Disponible en: http://seguridadinformaticasmr.wikispaces.com/TEMA 1-SEGURIDAD IFORMÁTICA>

Los planes apropiados varían de una empresa a otra, en función de variables como el tipo de negocio, los procesos involucrados, y el nivel de seguridad requerido. La planificación de la recuperación de desastres puede ser desarrollada dentro de una organización o se puede comprar una aplicación de software o un servicio. No es inusual que empresa invierta el 25% de su presupuesto de tecnología de la información de recuperación de desastres.

Sin embargo, el consenso dentro de la industria de DR es que la mayoría de las empresas todavía están mal preparadas para un desastre. Según el sitio de Recuperación de Desastres, "a pesar del número de desastres conocidos desde el 9/11, sólo el 50% de las empresas informan que tienen un plan de recuperación de desastres. De aquellos que sí lo tienen, casi la mitad nunca han puesto a prueba su plan, lo que equivale a no tener ninguno"[7].

3.5 INGENIERÍA SOCIAL

La Ingeniería Social es el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas. Éstas contemplan entre otras cosas: la obtención de información, el acceso a un sistema o la ejecución de una actividad más elaborada (como el robo de un activo), pudiendo ser o no del interés de la persona objetivo.
La Ingeniería Social se sustenta en un sencillo principio: “el usuario es el eslabón más débil”. Dado que no hay un solo sistema en el mundo que no dependa de un ser humano, la Ingeniería Social es una vulnerabilidad universal e independiente de la plataforma tecnológica. A menudo, se escucha entre los expertos de seguridad que la única computadora segura es la que esté desenchufada, a lo que, los amantes de la Ingeniería Social suelen responder que siempre habrá oportunidad de convencer a alguien de enchufarla[8].

La Ingeniería Social es un arte que pocos desarrollan debido a que no todas las personas tienen “habilidades sociales”. Aun así, hay individuos que desde pequeños han demostrado tener la aptitud y con un poco de entrenamiento convertirla en el camino ideal para realizar acciones maliciosas. Por ejemplo, hay crackers que en vez de perder horas rompiendo una contraseña, prefieren conseguirla preguntando por teléfono a un empleado de soporte técnico.
Formas de ataque

[7] SearhchDataCenter.com/es. Disponible en: <http://searchdatacenter.techtarget.com/es/definicion/Que-es-Plan-de-Recuperacion-de-Desastres-DRP>
[8] MOLIST, Mercè. Ingeniería Social Mentiras en la Red. Disponible en: <http://ww2.grn.es/merce/2002/is.html>

Las formas de ataque son muy variadas y dependen de la imaginación del atacante y sus intereses. En general, los ataques de Ingeniería Social actúan en dos niveles: el físico y el psicosocial. El primero describe los recursos y medios a través de los cuales se llevará a cabo el ataque, y el segundo es el método con el que se engañará a la víctima.

Las formas usadas a nivel físico son:

- **Ataque por teléfono**. Es la forma más persistente de Ingeniería Social. En ésta el perpetrador realiza una llamada telefónica a la víctima haciéndose pasar por alguien más, como un técnico de soporte o un empleado de la misma organización. Es un modo muy efectivo, pues las expresiones del rostro no son reveladas y lo único que se requiere es un teléfono.

- **Ataque vía Internet**. Desde que Internet se volvió uno de los medios de comunicación más importantes, la variedad de ataques en red se incrementaron tanto como la gran cantidad de servicios que existen en él. Los ataques más comunes son vía correo electrónico (obteniendo información a través de un phishing o infectando el equipo de la víctima con malware), web (haciendo llenar a la persona objetivo un formulario falso) o inclusive conversando con personas específicas en salas de chat, servicios de mensajería o foros.

- **Dumpster Diving o Trashing (zambullida en la basura**). Consiste en buscar información relevante en la basura, como: agendas telefónicas, organigramas, agendas de trabajo, unidades de almacenamiento (CD's, USB's, etc.), entre muchas otras cosas.

- **Ataque vía SMS**. Ataque que aprovecha las aplicaciones de los celulares. El intruso envía un mensaje SMS a la víctima haciéndola creer que el mensaje es parte de una promoción o un servicio, luego, si la persona lo responde puede revelar información personal, ser víctima de robo o dar pié a una estafa más elaborada.

- **Ataque vía correo postal**. Uno de los ataques en el que la víctima se siente más segura, principalmente por la fiabilidad del correo postal. El perpetrador envía correo falso a la víctima, tomando como patrón alguna suscripción de una revista, cupones de descuento, etc. Una vez que diseña la propuesta para hacerla atractiva, se envía a la víctima, quien si todo sale bien, responderá al apartado postal del atacante con todos sus datos.

- **Ataque cara a cara.** El método más eficiente, pero a la vez el más difícil de realizar. El perpetrador requiere tener una gran habilidad social y extensos conocimientos para poder manejar adecuadamente cualquier situación que

se le presente. Las personas más susceptibles suelen ser las más "inocentes", por lo que no es un gran reto para el atacante cumplir su objetivo si elige bien a su víctima.

Por otro lado, existen entornos psicológicos y sociales que pueden influir en que un ataque de ingeniería social sea exitoso. Algunos de ellos, son:

- **"Exploit de familiaridad".** Táctica en que el atacante aprovecha la confianza que la gente tiene en sus amigos y familiares, haciéndose pasar por cualquiera de ellos. Un ejemplo claro de esto ocurre cuando un conocido llega a una fiesta con uno de sus amigos. En una situación normal nadie dudaría de que ese individuo pudiera no ser de confianza. Pero ¿de verdad es de fiar alguien a quien jamás hemos tratado?

- **Crear una situación hostil**. El ser humano siempre procura alejarse de aquellos que parecen estar locos o enojados, o en todo caso, salir de su camino lo antes posible. Crear una situación hostil justo antes de un punto de control en el que hay vigilantes, provoca el suficiente estrés para no revisar al intruso o responder sus preguntas.

- **Conseguir empleo en el mismo lugar**. Cuando la recompensa lo amerita, estar cerca de la víctima puede ser una buena estrategia para obtener toda la información necesaria. Muchas pequeñas y medianas empresas no realizan una revisión meticulosa de los antecedentes de un nuevo solicitante, por lo que obtener un empleo donde la víctima labora puede resultar fácil.

- **Leer el lenguaje corporal**. Un ingeniero social experimentado puede hacer uso y responder al lenguaje corporal. El lenguaje corporal puede generar, con pequeños, detalles una mejor conexión con la otra persona. Respirar al mismo tiempo, corresponder sonrisas, ser amigable, son algunas de las acciones más efectivas. Si la víctima parece nerviosa, es bueno reconfortarla. Si está reconfortada, ¡al ataque!

- **Explotar la sexualidad**. Técnica casi infalible. Las mujeres que juegan con los deseos sexuales de los hombres, poseen una gran capacidad de manipulación, ya que el hombre baja sus defensas y su percepción. Probablemente suene asombroso, pero es aprovechar la biología a favor[9].

[9] SANDOBAL CASTELLANOS, Edgar Jair. Ingeniería Social: Corrompiendo la mente humana .Disponible en: <http://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana#_ftn1>

4. INGENIERÍA DEL PROYECTO

4.1 PLAN CONCIENCIACIÓN

El plan de concienciación es actualizado bajo el ciclo de mejoramiento continuo Planificar, Hacer, Verificar, Actuar (PHVA), en donde el ciclo que se está cerrando estaba constituido por tres elementos fundamentales; la concientización, un proceso de aprendizaje que buscó modificar actitudes y percepciones individuales, con el fin de desarrollar una idea de la importancia de la seguridad, así como demostrar los grandes problemas que conlleva el desconocimiento de las normas de seguridad. El segundo término fue el entrenamiento, cuyo objetivo fue la construcción del conocimiento con el propósito de aumentar las capacidades de una persona para desarrollar sus funciones de una manera más eficiente. La última etapa fue la educación, que se consideró una forma avanzada de entrenamiento, cuyo objetivo fue mejorar el conocimiento, destrezas y habilidades.

El desarrollo del nuevo plan de concienciación se basó en la experiencia del plan original teniendo en cuenta los puntos clave de cada una de las etapas (concienciación, entrenamiento y educación), concluyendo en un proceso de cuatro fases (Figura 4).

Figura 4. Estructura plan de concienciación

4.1.1 Fase 1 Diseño

En esta fase inicial se estructura el programa como tal, se evalúan las necesidades con base en la encuesta de seguridad informática realizada en el año 2014, se desarrollan las estrategias y finalmente se definen las prioridades de los temas a ser tratados en el plan.

4.1.1.1 Estructura del plan

El diseño de la estructura del programa se basó en la investigación realizada a lo largo del mes de Octubre de 2014, en donde se tomó como base el plan de

concienciación creado e implementado anteriormente, sobre el cual se modificaron varios aspectos de seguridad informática actual como son casos presentados a nivel mundial, tendencias tecnológicas actuales y adicionando la experiencia que se ha adquirido a lo largo de los últimos años en Caracol Televisión. Es así que se considera como resultado de la estructura del plan el presente documento.

4.1.1.2 Evaluación de necesidades

Como se mencionó anteriormente, la evaluación de necesidades resulta en primera instancia de la encuesta de Seguridad Informática realizada en el año 2014 y sobre la cual se concluyó que los principales temas sobre los que es necesario trabajar son la adopción por cada uno de los colaboradores del concepto que la responsabilidad de la Seguridad de la Información es responsabilidad de todas las personas, el tema de Back Ups por parte de los usuarios finales que manejan información sensible, Ingeniería Social, la Seguridad en el puesto de trabajo y especialmente el tema de Contraseñas Robustas. Por otro lado se identifican como nuevas necesidades los riesgos derivados de la evolución tecnológica que se viene presentado en los últimos años, las nuevas tendencias fomentan malos hábitos en los tema de seguridad de la información haciendo surgir nuevas formas de ataques a los sistemas y dispositivos entre otros.

4.1.1.3 Desarrollo de la estrategia

Teniendo en cuenta la cantidad de información a la cual los colaboradores están expuestos a diario, la principal estrategia es la de diseñar un plan de sensibilización atractiva y fácil de recordar para los colaboradores. En ésta nada puede quedar en el aire, todo deber ser debidamente planificado y elaborado, para poder realizar la divulgación y concienciación de forma masiva a Caracol Televisión de forma que se conozcan las nuevas responsabilidades.

Usando el humor como estrategia para llamar la atención de los colaboradores, se buscar lograr mayor recordación sobre el mensaje y generar una predisposición positiva hacia los temas persuadiendo, informando y divirtiendo mientras se crea simpatía hacia la temática. De esta manera la campaña de concienciación debe tener las siguientes finalidades:

- Informar al colaborador.
- Recordar la información suministrada.
- Persuadir para el uso de las buenas prácticas y recomendaciones.

La campaña se enfocará inicialmente en los siguientes tipos de humor:

- **Humor absurdo**: también conocido como humor superrealista, es un tipo de humor que se vale de las situaciones disparatadas o incoherentes para generar la risa en el público, su ingenio se basa en la irracionalidad. Es un humor totalmente alejado de la realidad pero que a la vez nos sumerge en lo esencial de ella. Ejemplo:

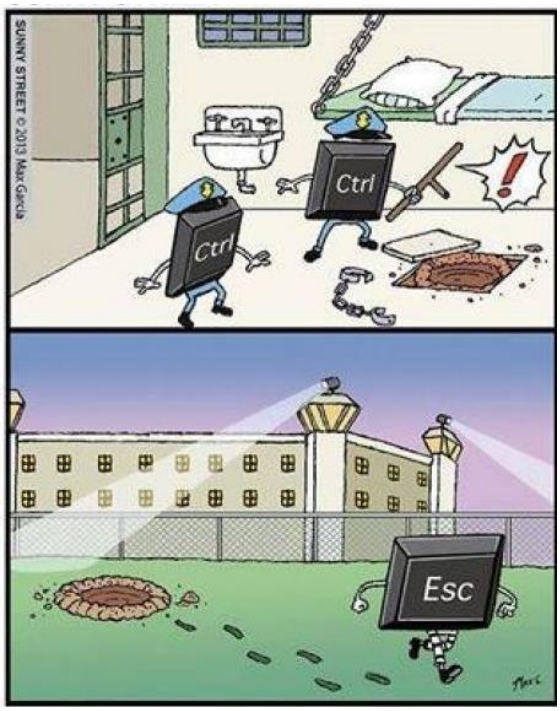

Figura 5. Humor absurdo[10]

- **Humor blanco**: es un tipo de humor que no contiene connotaciones ni denotaciones negativas, a saber: burla, ironía, machismo, cinismo, sexismo, racismo, etc. Es también llamado humor familiar, puesto que pueden disfrutarlo toda la familia, niños y adolescentes.

  Se basa en los siguientes elementos:
  - El factor sorpresa.
  - La calidad (o gracia) del intérprete (continente).
  - La calidad de lo expuesto (contenido).

  Un tipo de humor blanco es el chiste de salón, llamado así porque éste puede desplegarse en una fiesta o reunión sin riesgo de ofender ni escandalizar a ningún concurrente. Ejemplo:

[10] [Citado en Noviembre del 2014]. Disponible en <http://www.cuantarazon.com/866347/humor-absurdo>

Figura 6. Humor blando[11]

- **Humor gráfico**: se designa a una gama diversa de obras gráficas desde chistes de una sola viñeta y caricaturas hasta verdaderas historietas, tiras cómicas e incluso hojas enteras.

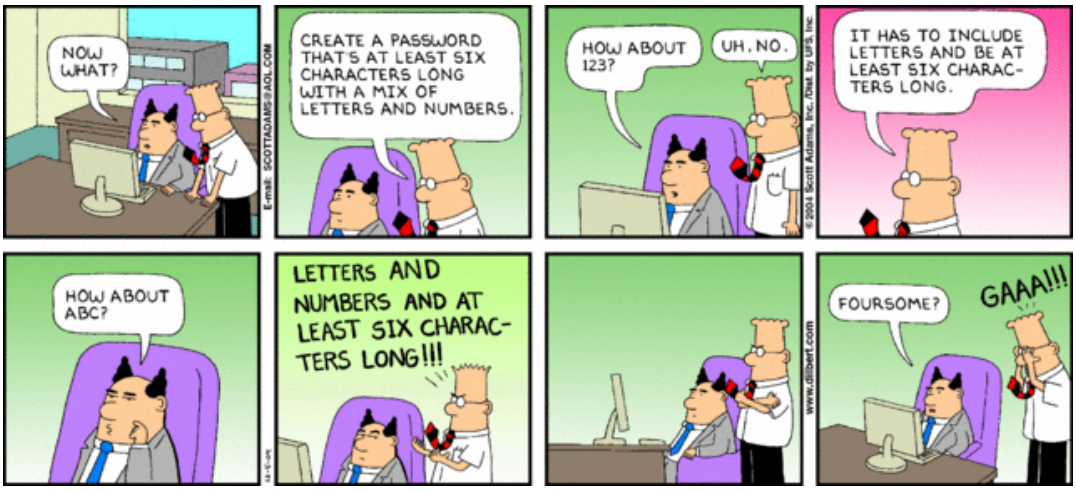

Figura 7. Humor grafico [12]

[11] [Citado en Noviembre del 2014]. Disponible en: <http://www.chistes21.com/chiste/23688_abrete-sesamo>

[12] [Citado en Noviembre del 2014]. Disponible en: <https://francoitgrc.wordpress.com/2012/02/10/concientizacion-en-seguridad/>

- **Humor hacker**: es un tipo de humor que comparten los expertos en computadoras (en particular, los hackers), que incluye cosas como parodias elaboradas de especificaciones, estándares, descripciones de lenguajes, etc.

Figura 8. Humor hacker[13]

4.1.1.4 Definición de prioridades

Con base en las necesidades identificadas anteriormente, la priorización de los temas que deben ser entregados a los colaboradores serán:

- Contraseñas Robustas
- Back Ups (especialmente con Office 365)
- Ingeniería Social
- Seguridad en el puesto de trabajo
- El mensaje correspondiente a que la Seguridad de la Información es responsabilidad de todos los colaboradores.

Los temas se tratarán mensualmente ya que con más espacio de tiempo es probable que los colaboradores dejen de lado la información que se les está entregando.

4.1.2 Fase 2 Desarrollo del material

En la fase anterior de diseño se estructuró como tal el plan de concienciación y lo orientó hacia dónde va a estar enfocado, de esta manera en la presente fase se

[13] [Citado en Noviembre del 2014]. Disponible en: <https://normantrujillo.wordpress.com/category/algo-de-humor/>

determina oficialmente la selección de los temas a ser tratados, así como su asignación mensual para ser trabajado.

4.1.2.1 Selección de temas

Con base en el desarrollo tecnológico tanto a nivel mundial como a nivel corporativo, el plan de concienciación debe abarcar una amplia gama de temas, elementos y aspectos tales como: continuidad de negocio, política de traiga su propio dispositivo (BYOD), Seguridad en la nube, el cumplimiento, correo electrónico, mensajería instantánea, redes sociales, la ética y la confianza, el fraude, la piratería, el error humano y los factores humanos, la gestión de incidentes, las amenazas internas, derechos de propiedad intelectual, malware, seguridad de red y de Internet, seguridad física, los secretos comerciales, entre otros.

Sin embargo algunos de los temas mencionados son relativamente estáticos, otros están evolucionando rápidamente y cada cierto tiempo algo novedoso aparece en el horizonte de seguridad. Por tal motivo se dejó un espacio en el ciclo actual para estar preparado a afrontar nuevas amenazas

De esta manera los temas a ser tratados serán:

- Contraseñas Robustas.
- Back Ups.
- Ingeniería Social.
- Seguridad en el puesto de trabajo.
- El mensaje correspondiente a que la Seguridad de la Información es responsabilidad de todos los colaboradores.
- Resumen del año anterior.
- Dispositivos móviles.
- Derechos de autor y software autorizado.
- Seguridad en la nube.
- Seguridad en el correo electrónico.
- Tema o tendencia que sea noticia en el 2015.
- Principales amenazas de temporada de fin de año.

4.1.2.2 Asignación Mensual

Durante la ejecución de la campaña de concienciación se trabajará a lo largo del año los diferentes temas de seguridad informática abordando los más importantes temas que deben ser reforzados y los temas de actualidad, cambiándolos mensualmente para evitar que el colaborador pierda el interés con los temas de

seguridad de la información. La organización de estos temas puede ser modificada dependiendo de los temas que se requieran trabajar ya sea para reforzar y/o mantener actualizador al colaborador. Cabe resaltar que el fin de estos temas es cambiar la mentalidad del colaborador referente a que no hay nada importante por proteger en el puesto de trabajo y en los dispositivos móviles y su vez indicando los beneficios que se consiguen al seguir las normas y recomendaciones expuestas.

4.1.3 Fase 3: Implementación del programa

Luego definir los temas a ser tratados para el año 2015 dentro del plan de concienciación, el siguiente paso es la implementación del programa a través de la creación y búsqueda del material a ser usado y su respectiva difusión.

4.1.3.1 Creación del material

De manera inicial la creación del material de concienciación estará enfocado en los elementos usados hasta la fecha, es decir, el protector de pantalla, el poster que se ubica en las carteleras de la compañía y el oponer que también puede ser usado como mensaje de correo electrónico a ser enviado a los colaboradores. Este material será creado de manera mensual en la última semana del mes previo a ser emitido.

Es de suma importancia que en el proceso de creación del material se incorporen los elementos creativos de tal manera que el plan evite ser monótono e ineficaz. La limitación del plan de sensibilización a un formato, modo o estilo es un corte suministro a aquellos que, por cualquier razón, no aprecian este enfoque concreto. Algunas personas responden mejor a las imágenes que a las palabras. Algunos prefieren que se les diga cosas, a otros les gusta que se muestre, otros tienen que descubrir por sí mismos. Algunos capturan los nuevos contenidos de forma rápida, mientras que otros necesitan más tiempo y reflexión o repetición. Un estilo formal y relativamente seco puede que se adapte a algunos, pero no para todos los materiales, temas y destinatarios.

4.1.3.2 Difusión

Para la divulgación del tema mensual hará uso de las siguientes estrategias de difusión:

- **Carteleras y volantes**

Cada día se maneja más tecnología pero no todos los colaboradores son usuarios de la misma. Pese a esto, la información presentada concierne a todos, de tal manera que mediante este tipo de medios se llega a los colaboradores que no tienen acceso a la tecnología y con quienes no se podría utilizar otro tipo de medios o mecanismos. Así mismo, para aquellos que tienen acceso a la tecnología, este medio se considera como un complemento informativo. Este tipo de material se sitúa en los diferentes puntos de las instalaciones en donde no pasará desapercibido.

- **Correo electrónico**

  Actualmente es el medio más usado dentro de Caracol Televisión debido a que en gran parte de los colaboradores manejan esta herramienta. Es eficaz, económico, ágil y permite alcanzar a las áreas o empleados que se encuentran geográficamente dispersos. A través de este medio se distribuyen copias de los poster de seguridad, posibles infografías, correos simulando ser Phishing, entre otros para reforzar la educación de los colaboradores sobre los diferentes temas.

- **Protector de pantalla**

  Al Mostrar mensajes a través del protector de pantalla, los colaboradores pueden leer y enterarse de forma fácil sobre los diferentes temas incluidos en el plan de concienciación, además que tiene una gran ventaja ya que es leído de forma inconsciente.

- **Premiación o reconocimiento**

  Constituyen una forma de despertar el interés y la sana competencia, que generalmente permiten alcanzar niveles muy altos de éxito y pueden contribuir a lograr un clima organizacional de cooperación y trabajo en equipo.

- **Capacitación**

  Uno de los principales espacios en donde es posible hacer conciencia en los colaboradores es en las capacitaciones de inducción para quienes ingresan a la Compañía a través de contrato por nómina. En este espacio se entrega un panfleto con los temas básicos de seguridad informática y a su vez es posible crear conciencia sobre los aspectos que deben tener en cuenta en el puesto de trabajo y en la organización generando así buenas prácticas.

- **Material POP**

  Busca generar una permanencia de la temática recurriendo a una gran variedad de objetos donde se puede imprimir o estampar información. Algunos

ejemplos de material POP son: Llaveros, relojes, calendarios, bolígrafos, mouse-pad, memorias USB, calcomanías, camisetas, pisa papeles de escritorios, bolsas de mercado o tiendas, agendas personales o de escritorio, tazas, vasos, entre otros.

4.1.4 Fase 4 Mantenimiento

4.1.4.1 Evaluación

Como parte del mejoramiento continuo del plan de concienciación, la evaluación del programa cobra suma importancia para ajustar los temas tratados mensualmente, así como para evaluar el desempeño de las técnicas, procedimientos y la metodología que fueron empleados para difundir los conceptos sobre seguridad informática e identificar los correspondientes puntos de mejora.

El proceso de evaluación estará enmarcado por la encuesta anual que se implementará hacia el mes de agosto de 2015 y que tiene como fin medir el nivel de efectividad de la campaña de concienciación, así como verificar la mejora en los temas identificados en las necesidades de la fase de Diseño y determinar las acciones requeridas a seguir, con base en las vulnerabilidades encontradas en el componente humano de los colaboradores de Caracol TV.

4.1.4.2 Indicadores

El indicador asociado al plan de concienciación es el referente a la percepción del servicio de seguridad informática, en donde se mide e identifica el número de usuarios satisfechos y muy satisfechos respecto al tema. El resultado de este indicador reflejará el nivel de sinergia entre los temas impartidos de manera mensual en cuanto a seguridad informática se refiere y el nivel de aprendizaje de los colaboradores en el tema, es decir, entre más se enseñe a los usuarios éstos tendrán un nivel más alto en percepción del servicio de seguridad informática.

El indicador se mide a través la suma de del porcentaje de usuarios satisfechos y del porcentaje de usuarios muy satisfechos. La meta a alcanzar el del 90% y su medición será anual.

4.1.5 Refuerzo

Con el propósito de reforzar el plan se concienciación con base a en el kit de concienciación de Incibe[14] se ha desarrollado una estrategia para apoyar las actividades a lo largo del año en la que se despliega una simulación de ataque dirigido dentro de Caracol Televisión basado en. De esta manera, se refleja el impacto generado en el plan de concienciación con los colaboradores y demostrando que tan vulnerables son, además de inculcarles que deben ser precavidos a la hora de abrir los archivos desconocidos.

Para ello se plantean dos formas de ataque: por correo electrónico y a través de memoria USB. Se utiliza ambos tipos de ataque antes o después de la sensibilización con los temas de Phishing y ataque a través de memorias USB, para poder evaluar el impacto generado de la campaña.

El simulacro busca crear cultura con respecto a la seguridad informática con la cual el colaborador pueda preocuparse por los archivos adjuntos recibidos por el correo electrónico de un usuario desconocido, tener precaución con los archivos que ejecuta, analizar con antivirus los archivos y las demás buenas prácticas para evitar los peligros que estas acciones puedan generar.

4.1.5.1 Correo electrónico con archivo malicioso adjunto

El primer tipo de ataque está basado en el envío de un correo electrónico con un archivo malicioso, el cual al ser ejecutado, muestra al colaborador una página Web informando el peligro que supone lo que acaba de hacer. Para ello, deben tener en consideración los siguientes puntos:

- Se utilizará una cuenta de correo electrónico ficticia pero cuyas características sean similares a las cuentas de correo de Caracol Televisión usando ya sea un dominio público o uno privado.

- Empleando la cuenta de correo, se enviará un correo electrónico masivo que será enviado a todos los colaboradores o a un número determinado de destinatarios que «participarán» en el simulacro sin su previo conocimiento. Con un pretexto previamente acordado, se pedirá a los colaboradores que ejecuten el archivo que se incluye en el correo electrónico.

- Es recomendable para dar credibilidad al correo, que éste lleve incluido en copia (campo CC) alguno de los cargos dentro de Caracol Televisión, antes

[14] Incibe. Manual de implantación del Kit de concienciación. Disponible desde internet en: <https://www.incibe.es/extfrontinteco/img/File/empresas/kit_concienciacion/incibe__kit_de_concienciacin__manual_de_implantacin.pdf>

debe obtenerse el permiso explícito de esta persona para incluirlo en la prueba. Además de adjuntar una firma.

- El asunto debe ser el título que lleguen los correos, por lo que debe ser lo más claro, llamativo y creíble posible.

- El archivo adjunto debe ser comprimido como .Zip para que no sea reconocido como un archivo malicioso.

4.1.5.2 Memoria infectada

El ataque está basado en la presencia de un archivo malicioso en varias memorias USB «extraviadas», los cuales al ser ejecutados, muestran al colaborador una página web advirtiéndole del peligro que supone lo que acaba de hacer. Para ello se deben tener las siguientes consideraciones:

- Es necesario adquirir las memorias USB donde irá almacenado el archivo «malicioso». Es recomendable que dicho archivo vaya acompañado de otro tipo de contenido totalmente inofensivo como Fotos o Documentación donde existen ciertos archivos genéricos como imágenes descargadas de internet, documentos PDF y/o documentos Excel o Word. Junto a ellos, se ubicará el archivo malicioso, siendo renombrado con algún nombre atrayente para cualquier colaborador como “secreto”, “material_privado” o “vacantes_2016”.

- El objetivo es que el colaborador se encuentre y utilice la USB o memoria localizada. Para ello, se deberá «abandonar» el dispositivo en una ubicación en la es más probable que un colaborador pueda encontrarlo. Algunos de estos lugares pueden ser:

    - Ascensor.
    - Baños.
    - Cafeterías o zonas de comida.
    - Pasillos de tránsito.
    - Escaleras.

- Es importante que el encargado de desplegar las memorias USB no sea detectado durante el proceso.
- Además informar al colaborador que recoja la memoria USB que lo correcto es la decisión de devolver el USB sin modificar su contenido.
- En el caso de que el colaborador o cualquier otro responsable devuelva la memoria USB a la Gerencia de Tecnología Informática, se le explicará la prueba y su finalidad, se le solicitará que no comente nada al resto de

compañeros de trabajo y se iniciará de nuevo el proceso, desplegando el USB en otra ubicación. Además, para ambos casos se recomienda explicar los motivos de la prueba a los colaboradores implicados.

4.1.5.3 Archivo malicioso

El archivo que se emplea en ambos ataques ya sea tipo Phishing o por medio de USB es un programa escrito en el lenguaje de programación por bloques o .bat conocido también de esta forma.

La única función de este archivo es abrir el navegador del colaborador o en el caso de que ya esté abierto, abrirle una pestaña directamente a una página web (URL pendiente) en donde se expongan los peligros de las acciones que acaba de realizar, así como las medidas que debe tomar o cualquier otra información pertinente para no provocar una posible infección de malware en la red de Caracol Televisión.

4.2 EJECUCIÓN DRP

El propósito de ejecutar y mantener actualizado el Plan de Recuperación de Desastre (DRP) es para lograr la continuidad de los servicios y aplicaciones críticas en el caso de indisponibilidad o falla total de las aplicaciones o del centro de procesamiento central y trabajo de Caracol Televisión. Los escenarios de falla fueron definidos y validados durante la etapa previa la cual se conoce como Definición de las Estrategias de Recuperación. Los procesos de negocio han sido soportados en uno o varios servicios y aplicaciones críticos a los que se hace referencia en el Manual. Los equipos, funciones, procedimientos y actividades descritos dentro del plan, deben ser usados como guía para la respuesta a escenarios de falla o situaciones de contingencia, en conjunto con las decisiones del Comité Directivo de Continuidad de TI y del Líder del DRP de Caracol Televisión El adecuado seguimiento de este plan soportará la recuperación oportuna de los servicios y aplicaciones definidos como críticos para el negocio.
Este plan se basa en una metodología que asigna funciones específicas a los miembros del comité y a los equipos de continuidad tecnológica; de esta manera cada persona o grupo de personas deberá seguir las instrucciones y roles descritos en las diferentes secciones del plan.

El plan depende de la disponibilidad, experiencia y conocimiento del personal del área de Tecnología Informática de Caracol Televisión, de los proveedores y terceros que operan la plataforma tecnológica, para apoyar los esfuerzos de recuperación, independientemente de las causas que den origen a la interrupción.

La intención de este plan no es recrear de forma idéntica los procesos y operaciones en estado normal.

4.3 NIVEL DE SEGURIDAD INTERNO

Como parte del plan de concienciación en seguridad informática en Caracol Televisión, a finales del 2014 se realizó la quinta encuesta de percepción, en la cual se busca medir los niveles de conocimiento en Seguridad Informática adquiridos por los colaboradores del Canal, luego de ser ejecutado dicho plan.

De igual forma se analizan los resultados obtenidos con los de años anteriores, con el fin de determinar fortalezas y debilidades en el proceso de concienciación, las temáticas que son necesarias para abordar y las estrategias para mejorar el proceso.

En ésta participaron colaboradores de diferentes cargos y áreas, siendo una muestra representativa del total de personas que trabajamos en Caracol Televisión. Entre los resultados obtenidos se puede evidenciar que:

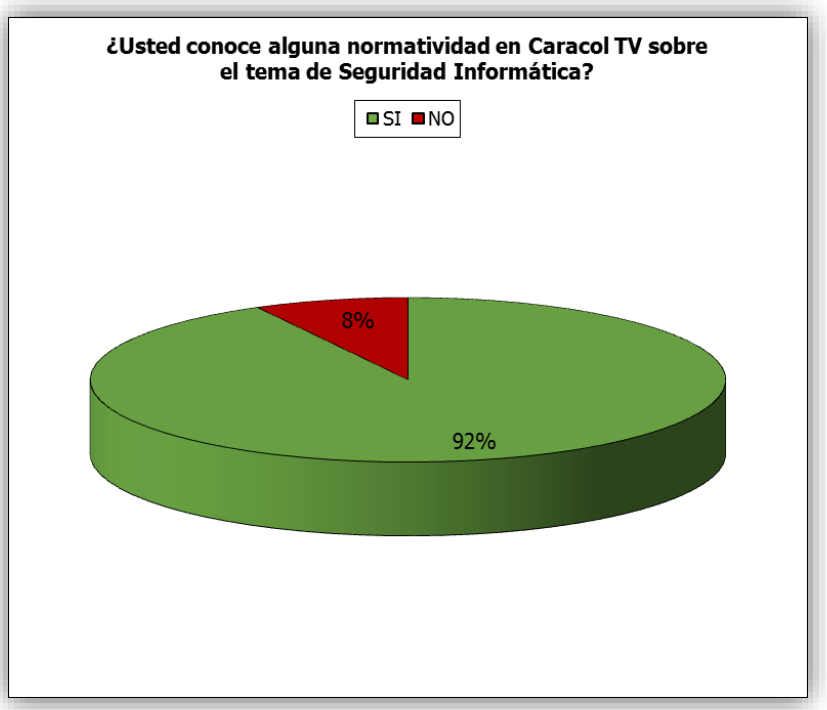

Figura 9. Normatividad organizacional

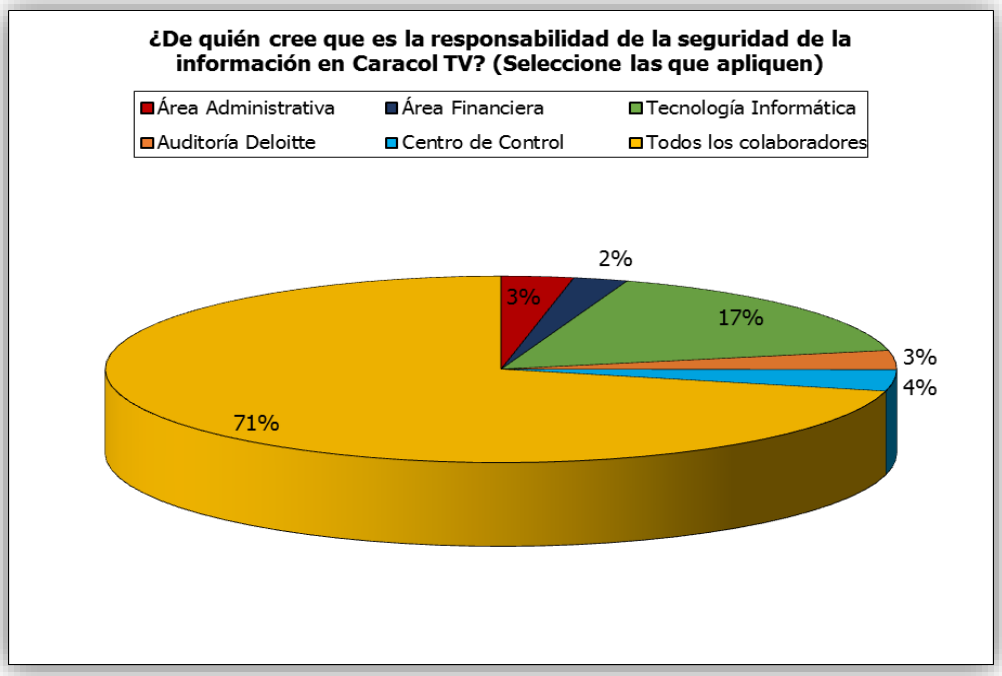

Figura 10. Responsabilidad de la seguridad informática

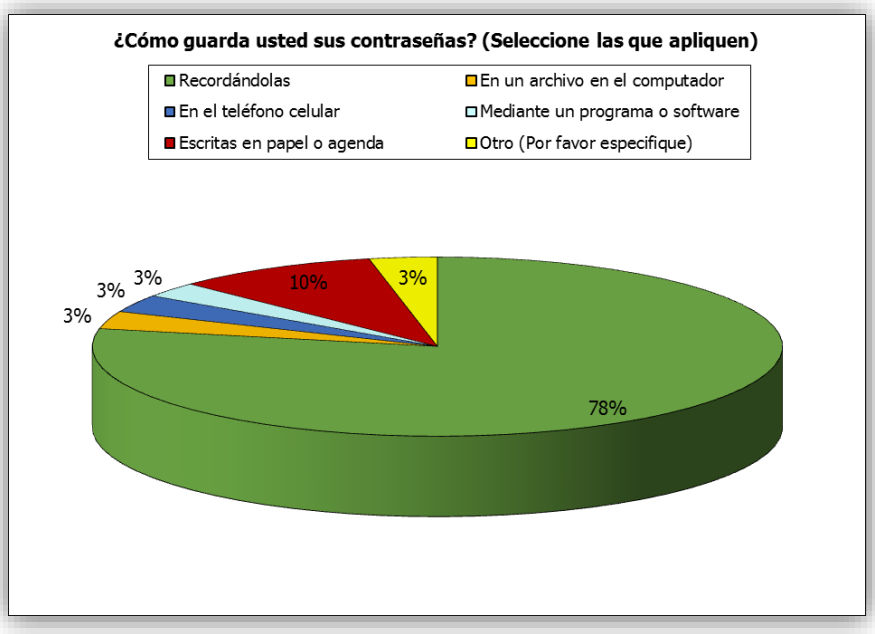

Figura 11. Manejo de contraseñas

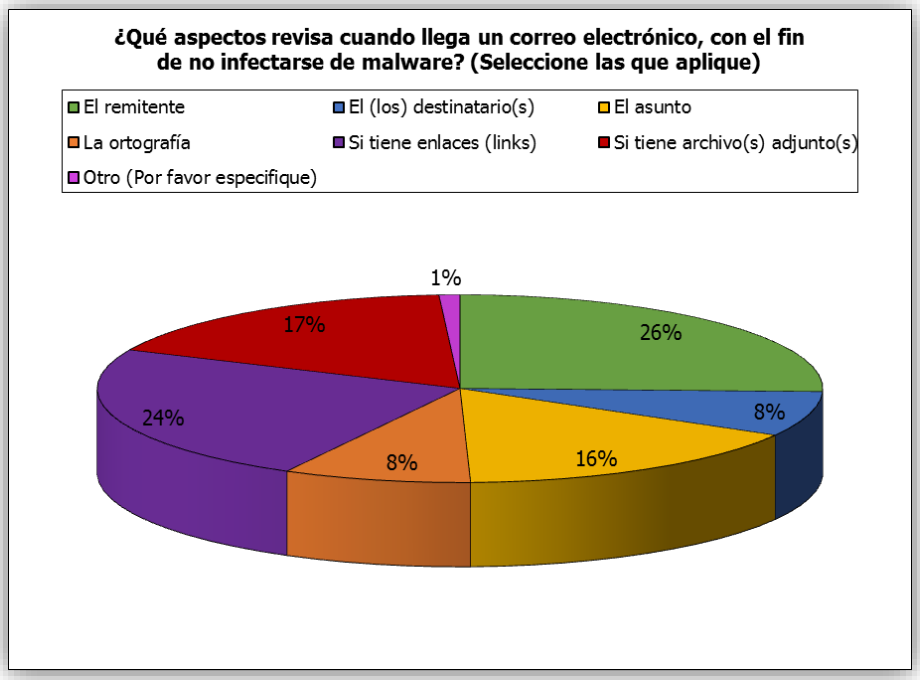

Figura 12. Identificación de correo malicioso

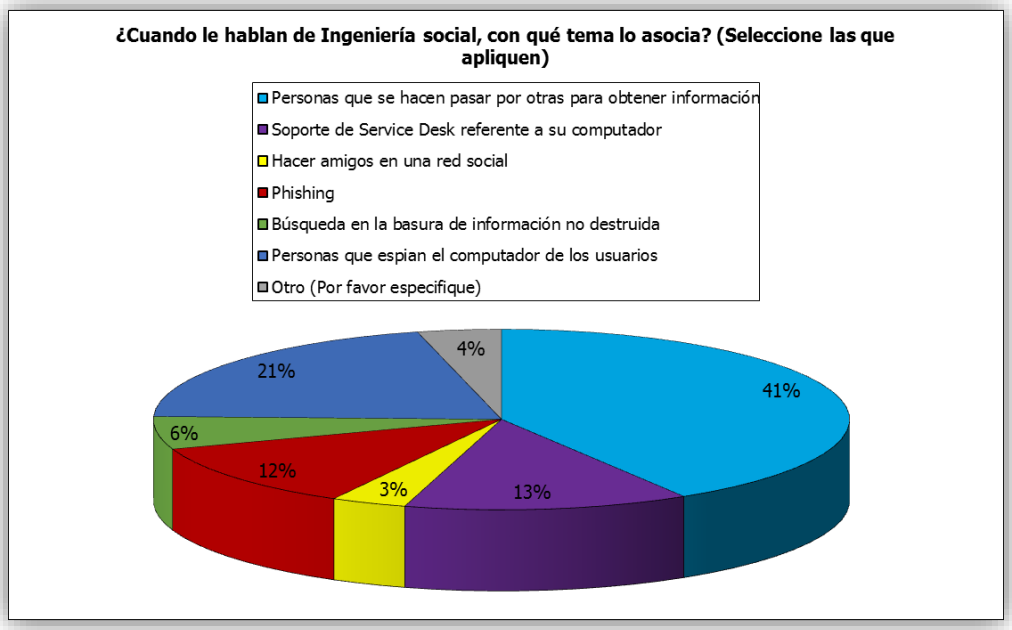

Figura 13. Ingeniería social

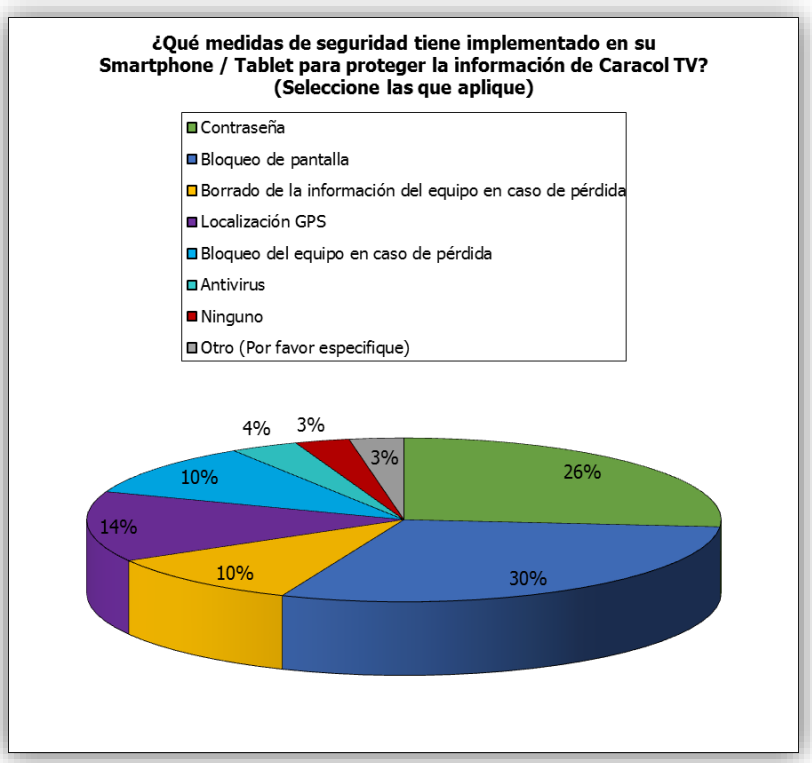

Figura 14. Seguridad dispositivos móviles

Teniendo como premisa el concepto de William Thomson que expresa "*Lo que no se define no se puede medir. Lo que no se mide no se puede mejorar. Lo que no se mejora, se degrada siempre.*", la comparación de los resultados anteriores con la del presente año ofrecerán los lineamientos con los cuales se deben trabajar para mejorar la forma de abordar los temas que se le entregan a los colaboradores en relación con la Seguridad Informática.

Comparando estos resultados obtenidos con los años anteriores se puede concluir que se debe seguir trabajando en la concienciación de los colabores para mejorar el conocimiento adquirido y reforzar las fallas en las prácticas de algunas prácticas, resaltar que es de responsabilidad de todos los colaboradores la seguridad de la información, se debe aumentar las prácticas para salvaguardar la información en los computadores, dispositivos móviles y otras tecnología que pueda almacenar y procesar la información, finalmente comunicar a los colaboradores sobre los nuevos riesgo y engaños creados por la ingeniería social para no caer en dichas trampas.

4.4 GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

Con el acelerado avance de la tecnología y la adaptación de la información a las nuevas tendencias tecnológicas, los criminales buscan acceder a los sistemas explotando las nuevas vulnerabilidades que se encuentran en internet hoy en día. Para evitar ingresos no autorizado a los sistemas es necesario responder a estos eventos de una manera eficaz y oportuna

Un incidente de seguridad informática puede ser originado dentro o fuera de la Caracol Televisión, así como envolver entes externos e internos, y puede variar en severidad. Éstos involucran violaciones a las políticas y normas de Caracol Televisión, acceso no autorizado a la información, alteración de la integridad de un sistema/servidor, interrupción o daño de la disponibilidad de servicios, espionaje, exploración no autorizada de la red, alteración o modificación del sitio Internet, ataques conocidos: Denegación de Servicio (DoS/DDoS) o malware, destrucción de datos, fraude, hurto, entre otros. Así mismo los eventos hacen parte de las evidencias recolectadas luego de un incidente de seguridad. Entre otros se encuentra: El reinicio de un sistema, creación de nuevas cuentas de usuario, cambio de claves de acceso en cuentas existentes, modificación a las protecciones definidas, creación de programas, reemplazo o modificación de archivos, creación de archivos o cuentas ocultas, la caída de un sistema.

De esta forma se abarca el tema relacionado a la gestión de incidentes de seguridad informática en dado caso que se presenten en las instalaciones de Caracol Televisión, teniendo en cuenta los diferentes acontecimientos que un usuario identifique en su labor diaria.

Para proporcionar una solución eficaz y oportuna del incidente que afectan a los colaboradores y los medios informáticos, se maneja una clasificación de los incidentes. Para hacer una gestión adecuada, todos los incidentes deben ser clasificados teniendo en cuenta factores:

- Naturaleza del evento.
- Sistemas afectados.
- Numero de sistemas involucrados.
- Impacto organizacional.

En la siguiente tabla se muestra un modelo de referencia para la categorización del incidente, donde se clasifican los incidentes:

Clase de Incidente	Tipo de Incidente	Descripción
Ataques	Ataque dirigido	Se considera un ataque dirigido a aquel donde el(los) individuo(s) o la organización afectada(o) están intencionadamente elegidos. Este tipo de ataques pueden incluir otras clases y tipos de ataques (spam con código dañino, APT, SMTP Flood[15], ingeniería social, etc), pero dada su criticidad, deben considerarse como un tipo independiente si en la fase de clasificación se tienen indicios claros de que son dirigidos.
	Modificación del sitio web	Vulnerabilidades explotadas con éxito en los sistemas de alojamiento (servidor web) o en las aplicaciones que permiten a un atacante modificar contenidos y páginas web. Estos ataques pueden involucrar la inserción de enlaces a sitios maliciosos y/o añadir contenidos que contienen el mensaje (políticos, difamatorios, etc).
Código dañino	Infección extendida	Un virus, gusano, caballo de troya, rootkit, script, etc. que infecta exitosamente a un conjunto amplio de sistemas y en donde han fallado las medidas de detección y/o contención

[15] El envío masivo de mensajes de correo electrónico a grandes listas de usuarios de forma continua, se provoca la saturación de los servidores de correo destino o intermedios.

		establecidas.
	Infección única	Malware que solo afecta a un dispositivo, usuario o sistema.
Denegación del servicio (DoS/DDoS)	Exitosa	El intento exitoso de ataque DoS/DDoS (Denegación de Servicio Distribuida) para afectar un servicio o sistema. Se puede conseguir a través del uso de vulnerabilidades presentes en la infraestructura o, más comúnmente, mediante el envío masivo de grandes cantidades de tráfico y/o peticiones. El resultado es que el sistema no es capaz de responder a las peticiones de servicio de los usuarios legítimos.
	No exitosa	El intento no exitoso de un ataque DoS/DDoS. El ataque ha sido eliminado o mitigado por los controles establecidos, y no se ha producido pérdida significativa de servicio.
Acceso no autorizado, robo, alteración o filtración de información	Acceso no autorizado	Se produce cuando un atacante obtiene acceso lógico o físico a un equipo, sistema, aplicación, dato o cualquier recurso informático corporativo. El origen del ataque puede ser tanto externo como interno.
	Robo o pérdida de equipos o medios informáticos	Robo o pérdida de equipamiento su ministrado por TI, como por ejemplo

		computadores portátiles, cintas, memorias USB, etc.
	Alteración de la información	Modificación de datos que comprometa la confidencialidad, disponibilidad e integridad.
	Filtración de información	Pérdida o filtración de datos que comprometan la seguridad e integridad de los sistemas y los procesos internos de Caracol Televisión. Por ejemplo credenciales, documentación, información de los colaboradores, etc.
Pruebas y reconocimientos	Pruebas no autorizadas	Cualquier actividad que busque acceder o identificar sistemas, puertos, aplicaciones, servicios, cuentas de usuarios o información de los sistemas para un uso ilícito posterior.
	Alarmas de sistemas de monitorización	Son aquellos eventos de seguridad (en el firewall, antivirus, correo electrónico, etc.) que puedan ser significativos pero que no permitan clasificar al incidente en alguna otra categoría establecida.
Daño físico	Daños o cambios físicos no autorizados a los sistemas	Se produce cuando un individuo sin autorización (interno o externo) consigue acceso físico a los equipos y/o instalaciones, y realiza cambios, instalación, modificación y/o daños no autorizados.

Abuso de privilegios y usos inadecuados	Abuso de privilegios o de políticas de seguridad de la información	Un individuo que realiza una violación de los sistemas y redes de Caracol Televisión.
	Infracción de derechos de autor o piratería	La copia o el uso no autorizado o prohibido de obras cubiertas por las leyes de derechos de autor, como el derecho de copia, de reproducción o el de hacer obras derivadas.
	Uso indebido de la marca	Uso de elementos identificativos de la elementos de la marca corporativa (logos, imágenes, etc.) en cualquier intento fraudulento para adquirir información confidencial, como usuarios, contraseñas o cualquier otra información personal que permitan al atacante hacerse pasar por la organización legítima víctima del incidente. Entrarían en esta categoría ataques de Phishing en que Caracol Televisión es la víctima en tanto que es su imagen la que se está siendo empleada para engañar a los individuos. No se corresponderían a esta categoría ataques en que el usuario recibe mensajes de Phishing de otras organizaciones (por ejemplo bancos o redes sociales).

Figura 15. Clasificación incidente informático.

Una vez es clasificado el incidente se procede a crear el plan de trabajo para su mitigación y neutralización de la amenaza definiendo las acciones correctivas para restablecer los sistemas y servicios afectado. Conforme a las acciones establecidas se realiza un seguimiento de la situación en todo momento para evaluar el estado de los sistemas y aplicaciones involucrados, y definir procesos a realizar según sean los resultados obtenidos.

Luego de ser solucionado el incidente informático se efectúa una reunión con los directivos de Tecnología Informática y de ser necesario otros directivos fuera del área para analizar el evento ocurrido y sacar las respectivas conclusiones, futuras acciones a tomar, establecer las sanciones o procedimientos a tomar para los distintos involucrado.

Finalmente se documenta todo el incidente indicando información del evento, medidas y soluciones realizadas, conclusiones, medidas tomadas, lecciones aprendidas y cualquier otra información que sea necesario para el tratamiento de futuros incidentes similares y se almacena con la demás información y/o materiales relacionados con el evento.

4.5 AMENAZAS

La seguridad informática busca minimizar todas las amenazas y riesgos que están presentes diariamente que afecta los recursos tecnológicos de las organizaciones, dentro de las amenazas se pueden encontrar ataques informáticos a servidores y aplicaciones, robo y manipulación de la información, penetración no autorizada a los sistemas, escalamiento de privilegios, manipulación de la estructura tecnológica, entre otras. Estos temas no son tomados en cuenta por parte del personal de las empresas ya sean colaboradores o directivas, pensando que no es un deber para ellos y es la responsabilidad solamente de TI o del oficial de seguridad informática.

Al promover en los colaboradores de Caracol Televisión sobre *la seguridad de la información es comportamiento y no un departamento* se gusta promover una solidad cultura de ciberseguridad, que maximice la protección de los recursos informáticos y minimicen los riegos a los que pueden exponer al abrir un correo, entrar a un sitio web, conectar una memoria USB, etc. Con este motivo se investiga los posibles peligros que se genera con la aparición de nuevas vulnerabilidades y técnicas de explotación de las debilidades que afectan a los distintos sistemas y aplicaciones.

Las personas malintencionadas desarrollan métodos para aprovechas las vulnerabilidades de los sistemas y crean nuevas amenazas como lo son las APT

(amenaza persistente avanzada), creación de nuevas cepas de malware como son el Cryptolocker, Chthonic, BlackPos y Wireluker. Asimismo el desarrollo de métodos más eficaz para el robo de información entre las que se destacan las campañas de Phishing, Darkhotel, Soaksoak, Regin, Dridex, Machete, Botnet, RFD, BadUSB etc. Explotando las vulnerabilidades existentes para acceder a la infraestructura y dispositivos tecnológicos de forma que consigue la manipulación del sistema logrando el propósito preestablecido de la persona malintencionada.

Tantas son las amenazas que afectan a los sistemas informáticos que aprovechan las nuevas vulnerabilidades, que se está desarrollando una "carrera armamentista" entre las empresas especializadas en seguridad informática y piratas informáticos, protegiendo y explotando los sistemas. Los proveedores de soluciones informáticas buscando mitigar las amenazas que son creadas y minimizan el impacto generado. Empresas como Panda, IBM, FireEyes, Fortinet, SourceFire Kaspersky, entre otras, crean herramientas para aumentar la protección de los sistemas en las organizaciones entre las que se pueden destacar las IPS (Detector de intrusos), soluciones de Cifrato, Backup, Antimalware, administración de eventos y logs de seguridad, filtrado web, protección de correo y Firewall de nueva generación, accesibles para pequeñas, medias y grandes empresas, estas organizaciones y asociados invitan al personal encargado de los oficiales de seguridad informática de diferentes entidades a conferencias y reuniones para dar a conocer las nuevas soluciones de seguridad informática enfocando a cómo mejora la gestión de incidentes y procesos internos.

Además de la implementación soluciones tecnológicas enfocadas a la seguridad de los recursos informáticos es necesario informar a los colaboradores de las nuevas amenazas a las que pueden estar expuestos ya sea por medio de un macro en un documento o por el robo de información a través de líneas telefónicas o personalmente. Conforme con la aparición de las amenazas y el impacto que genera en Colombia y/o Latinoamérica se analiza la posibilidad de comunicar sobre la amenaza, cómo es difundida y mencionando las características principales para identificarla.

4.6 ANÁLISIS DE VULNERABILIDADES

La seguridad informática tiene entre sus principales tareas el análisis de vulnerabilidades que son los puntos débiles en los sistemas y aplicaciones que maneja principalmente activos de la información y amenazan la integridad disponibilidad y confidencialidad, la cual indica que el activo tecnológico es susceptible a recibir un daño a través de un ataque, ya sea intencional o accidental. Con el fin de aumentar la seguridad en los sistemas y asegurar los

recursos que pueden estar afectados ante un ataque informático por parte de una persona malintencionada interna o externa a la organización.

El análisis de vulnerabilidades es una actividad imprescindible para garantizar los activos informáticos, dentro de los cuales se pueden encontrar los servicios, sistemas, aplicaciones, Firewalls, puestos de trabajo, etc. Con el propósito de proteger la infraestructura se desarrolla un ciclo de 4 pasos: Análisis, Investigación y Confirmación, Simulación, Implementación.

4.6.1 Análisis.

En esta fase inicial se examina la integridad de los sistemas con la ayuda de una herramienta para la detección de vulnerabilidades y de ser necesario se realiza con ayudar de auditoria externas, identificando los elementos potenciales que pueden originar un incidente de seguridad en un futuro cercano o lejano.

4.6.2 Investigación y confirmación.

Una vez es identificado se examina con las base de datos de vulnerabilidades del proveedor identificando el CVE (common vulnerabilities and exposure) y comparando las base de datos de Caracol Televisión además de los manuales de las aplicaciones y servicios internos para validar si dicha vulnerabilidad afecta a los activos tecnológico del Canal.

4.6.3 Simulación

Luego ser confirmada la vulnerabilidad se procede a instalar el parche correctivo respectivamente en un ambiente virtual para validar el comportamiento de las aplicaciones internas y sistemas de modo que no afecte su operatividad.

4.6.4 Implementación

Luego de validar que el respectivo parche de seguridad funciona al 100% y no tiene problemas de compatibilidad se procede a programar e instalar en los distintos equipos en los que son necesarios. Mensualmente se desarrolla este proceso acorde a la publicación de los parches de seguridad más recientes.

4.7 DESCRIPCIÓN DE LA SITUACIÓN ACTUAL

En la actualidad la información manejada por parte de los colaboradores de Caracol Televisión sin importar su clasificación está protegida con procedimientos, controles, normas y políticas desactualizadas que no son los adecuados para asegurar como es debida la información obteniendo como resultados incidentes de seguridad informática y es producido por las nuevas tendencias tecnologías que se presentan año tras año como lo son los dispositivos móviles y cloud computing.

4.8 REQUERIMIENTOS DE LA INFORMACIÓN

En Caracol Televisión se debe establecer, implementar, monitorear, conservar y actualizar continuamente la normatividad y los procedimientos internos para garantizar la operación en los distintos servicios y aplicaciones, para minimizar los riesgos que enfrentan. Entre los principales requerimientos se encuentra:

- Implementar el mejoramiento continuo en la gestión de la seguridad de la información en la TI.
- Identificar y gestionar las amenazas y vulnerabilidades para mitigar los posibles impactos que pueden afectar la normal actividad de TI.
- Asegurar la continuidad de las operaciones de los servicios y Aplicaciones Corporativas basados en una infraestructura homogénea, escalable, flexible y segura acorde a las necesidades de la Compañía.
- Incrementar el nivel de conocimiento en ciberseguridad todos los colaboradores de Caracol Televisión.
- Garantizar el seguimiento de las distintas directrices implementadas por el TI.
- Definir el alcance de la seguridad informática.
- Especificar una metodología adecuada para el análisis y gestión de incidentes informáticos.
- Identificar los controles que se deben actualizar.

- Implementar controles adecuados para garantizar la confidencialidad, integridad y disponibilidad de la información.

- Crear una metodología adecuada para la concienciación de los colaboradores de Caracol Televisión.

- Desarrollar conciencia en los colaboradores de Caracol Televisión en seguridad informática.

- Establecer controles para la seguridad física y perimetral.

4.9 DESCRIPCIÓN DEL SISTEMA.

Caracol Televisión S.A. es una compañía perteneciente al Grupo Empresarial Valorem el cual tiene proyectado la implementación de SAP para el procesamiento de la información de forma integral, al igual que optimizar procesos internos. Se basa en el concepto de combinar todas las actividades de negocio y los procesos técnicos de Caracol Televisión en una solución informática simple, integrada, robusta y fiable.

Debido que en el sistema actual tiene implementado solamente el Antivirus, Firewall y un gestor de páginas web, la seguridad que brinda para proteger la información es mínima contras las nuevas amenazas como lo son las APTs, los nuevos métodos de extracción de datos, la evolución de las técnicas maliciosas, la ingeniera social, nuevos métodos de infección, el desarrollo de códigos maliciosos, entre otros. Un individuo interno o externo malintencionado con conocimientos informáticos suficientes puede ingresas en los sistemas de Caracol Televisión y robar y/o alterar la información encontrada, filtrar información, suplantar identidades, dañar los sistemas, etc.

5. EVALUACIÓN ECONÓMICA DEL PROYECTO

5.1 RIESGO EN FASE DE ANÁLISIS

- Existan directrices necesarias o importantes que quedan por fuera y puedan tener un gran impacto.

5.2 RIESGO EN FASE DE DISEÑO

No se desarrolla la documentación, procedimientos y políticas necesarias.

- No se crea una metodología adecuada.
- Se tiene información incompleta o nula para el desarrollo de las actividades.

5.3 RIESGO EN FASE DE CODIFICACIÓN

- Se dejen huecos en las políticas que puedan ser aprovechados.
- Se creen medidas de seguridad inadecuadas o desactualizadas.

5.4 RIESGO EN FASE DE PRUEBAS

- El escenario de prueba no es lo más aproximado a la realidad.
- No se examina todos los escenarios de éxito y error del sistema teniendo en cuenta los procesos que el usuario realizar en el sistema.
- Las pruebas no se realizan de forma correcta.

5.5 RIESGO EN FASE DE IMPLEMENTACIÓN

- No se absorba bien el mensaje trasmitido por parte de los colaboradores.
- Inexactitud de las pruebas realizadas.
- Mala planificación que tiene como resultado la pérdida de la disponibilidad de la información y los sistemas.
- No se obtenga la certificación o exista un retraso en el cronograma.
- Incumplimiento o descuido de las políticas establecidas.

5.6 RIESGO EN FASE DE MANTENIMIENTO

- Desconocimiento parcial o total del(los) sistema(s) y aplicación(es).
- Falla en programación del mantenimiento.
- Falla al identificar las vulnerabilidades del(los) sistema(s).

5.7 RIESGOS EN GENERAL

- Falla al clasificar la información y los activos.
- Falla al identificar los activos críticos, confidenciales y sensibles dentro de la organización
- Falta de compromiso por los altos directivos de las políticas de seguridad informática.
- Dificultad al identificar errores del(los) sistema(s).
- Problemas al identificar las vulnerabilidades de seguridad informática (Bug´s, 0-Day, warning, etc).
- Debilidad al sensibilizar sobre la implementación de las directrices en los sistemas a los colaboradores.
- Determinar la ocurrencia de los incidentes.
- Falla al clasificar los incidentes de seguridad.
- Acceso indebido o no autorizado a la información.

6. PRESUPUESTO DETALLADO

Los costos depende de la cantidad de material y trabajo que se deba realizar, a continuación se describe las derivaciones económicas de la aplicación de la norma ISO/IEC 27001:2013 categorizando el tipo de costo:

6.1 COSTES RELACIONADOS CON LOS CAMBIOS ORGANIZACIONALES

- Difundir y aumentar la concienciación de los colaboradores en los temas de la seguridad informática.
- Actualizar y crear normas, procedimientos, guías, políticas, etc.
- Pérdidas generadas por el despido de un colaborador por incumplir las normas.

6.2 COSTES DE DISEÑO Y DESARROLLO

- Actualizar la documentación referente a la seguridad de la información.
- Creación de nuevos procedimientos para asegurar la información.
- Actualizar la documentación y los procedimientos en los diferentes controles de la gestión de incidentes informáticos.
- Diseño de metodología adecuada para concientizar a los colaboradores.

6.3 COSTES DE LA IMPLEMENTACIÓN

- Actualizar y complementar los controles existentes para cumplir con la norma ISO/IEC 27001.
- Actualizar la certificación.
- Seguimiento y visitas del auditor.
- Mantenimiento de las políticas, normas, guías, directrices, etc., de la seguridad de la información.
- Mantenimiento procedimiento del DRP.
- Material para la concienciación e inducción
- Revisión y mantenimiento anuales de las directrices de seguridad informática para el cumplimiento de la norma ISO/IEC 27001.
- Seguimiento de las políticas de seguridad

6.4 COSTO DE INFRAESTRUCTURA FÍSICA

- La norma ISO/IEC 27001 no está orientada a la instalación de equipo tecnológico o de infraestructura, sino a aspectos netamente organizacionales.

7. BENEFICIOS DE LA IMPLEMENTACIÓN

Los beneficios proporcionados por la actualización de la norma ISO/IEC 27001 son principalmente con relación a la confidencialidad, disponibilidad e integridad de los datos para los colaboradores de Caracol Televisión de igual forma a nivel organizacional se pueden encontrar:

7.1 OPERACIONALES

- Se conserva un plan actualizado para la continuidad de negocios en caso de un incidente sin importar su magnitud con el propósito de garantizar la continuidad y disponibilidad.
- Se mejora la seguridad de la información en los datos privados y corporativos.
- Se está preparados para entrar en contingencia debido algún incidente informático.

7.2 DE GESTIÓN

- Establece una metodología de gestión de seguridad informática clara y estructurada.
- Mejora la gestión de los incidentes de seguridad informática.
- Evita la fuga de la información.
- Mejora la seguridad de la información interna.
- Optimiza la gestión de la información en los sistemas internos.

7.3 ESTRATÉGICOS

- Apoyo en el desarrollo empresarial.
- Implementa las nuevas innovaciones a la organización.
- Resguarda la información de una forma más óptima.
- Reduce la posibilidad y el impacto generado con un incidente de seguridad
- Se minimizan de costos por incidentes informáticos.
- Aumenta la seguridad de la información en base a la gestión de procesos en vez de comprar equipos tecnológicos.

7.4 DE INFRAESTRUCTURA

- Fomenta la cultura de ciberseguridad.

7.5 DE IT

- Aumenta la seguridad en los procesos.
- Reduce los riesgos generados por fuga de información.
- Reduce los riesgos frecuentes con respecto a la información.

8. ALCANCES DEL PROYECTO

El alcance de este proyecto abarca los servicios prestados directamente a los colaboradores a través de la Dirección de Operaciones de TI y de la Dirección de Proyectos y Aplicaciones. Adicionalmente cubre las funciones de soporte a la gestión del área tales como Planeación estratégica de TI, Definición y mantenimiento de la Arquitectura de TI, Evaluación y priorización de proyectos, Indicadores de TI, Gestión de los recursos humanos y económicos de TI y Seguridad de TI.

9. LIMITACIONES DEL PROYECTO

- Seguimiento de las directrices creadas y establecidas.
- Apoyo de Altos Directivos (si los jefes apoyan los usuarios los siguen).
- Presupuesto para la motivación en la concienciación.
- Cumplimiento continúo de las normas por parte del personal.
- Capacitación de los practicantes y pasantes.

10. CRONOGRAMA.

ACTIVIDAD	Mese																	
	Octubre					Noviembre				Diciembre					Enero			
	Semanas																	
	1	2	3	4	5	1	2	3	4	1	2	3	4	5	1	2	3	4
Enfoque documentación seguridad informática																		
Revisión de la ISO 27001:2013																		
Revisión de documentación de seguridad informática de Caracol Televisión.																		
Análisis resultados de la V encuesta de seguridad informática.																		
Revisión y exposición de los resultados.																		
Actualización de guías y nomas de seguridad informáticas																		
Indagación y Creación de nuevas guía y normas de seguridad informática.																		
Recolección y análisis e la información del análisis de vulnerabilidades de TI y clasificación por tipo y criticidad																		
Enfoque Plan de Recuperación de Desastres (DRP)																		
Actualización del manual del DRP																		
Planeación del manual del DRP																		
Preparación del material para la prueba																		

Recolección de la información durante la prueba																		
Creación de documentos de planes de acción DRP																		
Actualización del manual del DRP																		
Enfoque seguridad informática en TI																		
Control ISO27002 11.1.1: Perímetro de seguridad física																		
Control ISO27002 11.1.2: Controles físicos de entrada																		
Control ISO27002 11.1.3: Seguridad de oficinas, despachos y recursos																		
Control ISO27002 11.1.4: Protección contra amenazas externas y ambientales.																		
Control ISO27002 11.2.1: Emplazamiento y protección de equipos.																		
Control ISO27002 11.2.2: Instalación de suministros																		
Control ISO27002 11.2.3: Seguridad del cableado																		
Control ISO27002 11.2.5: Salida de activos fuera de las dependencias de la organización																		
Control ISO27002 11.2.8: Equipo informático de usuario desentendido																		

Control ISO27002 12.1.4: Separación de entorno de desarrollo, prueba y producción																	
Control ISO27002 12.2.1: Controles contra el código malicioso																	
Control ISO27002 12.4.2: protección de los registros de información																	
Control ISO27002 12.5.1: instalación de software en sistemas de producción																	
Control ISO27002 13.1.1: Controles de red																	
Enfoque Gestión de incidentes de seguridad informática																	
Control ISO27002: 16.1.1 Responsabilidades y procedimientos																	
Control ISO27002: 16.1.2 Notificación de los eventos de la seguridad informática																	
Control ISO27002: 16.1.3 Notificación de puntos débiles de seguridad																	
Control ISO27002: 16.1.4 Valoración de eventos de la seguridad informática y toma de decisiones																	
Control ISO27002: 16.1.5 Respuesta a los incidentes de seguridad																	
Control ISO27002:																	

16.1.6 Aprendizaje de los incidentes de seguridad de la información																		
Control ISO27002: 16.1.7 Recopilación de evidencias																		
Enfoque Plan de concienciación																		
Revisión y actualización de la documentación del plan de concienciación																		
Indagación temática																		
Preparación del material																		

11. RECOMENDACIONES

- Es necesario incentivar el valor de la información sin importar su tamaño o contenido.
- Predisponer al personal de TI que los procedimientos de seguridad informática no son para poner más trabajos en las actividades diarias.
- Fomentar y divulgar el uso de las buenas prácticas para asegurar la información.
- Dar prioridad a los parches de seguridad a los sistemas operativos de Linux y Mac como se efectúa en Windows, dependiendo la criticidad de la vulnerabilidad.
- Es importante definir cuáles son las directrices que se deben actualizar anualmente.
- Se debe aumentar el material de apoyo para el plan de concienciación para que sea más fácil entender las distintas temáticas sé que se manejan.

12. CONCLUSIONES

Entre las principales conclusiones que se puede obtener se encuentra:

- Es necesario seguir trabajando para hacer conciencia sobre la seguridad de la información sin importar si son nuevos, antiguos o altos directivos debido que la seguridad es de responsabilidad de todos los colaboradores.

- De la misma manera se debe reforzar y dar conocer la normatividad de Caracol TV referente a los temas de seguridad de la información, tanto para los colaboradores internos, como para los que ingresan al Canal.

- Se debe conocer y clasificar la información manejada dentro de Caracol Televisión para saber el grado de riesgo que puede generar la peritada, robo o filtración y manipulación indebida de la información.

- La seguridad informática debe tratarse como un problema de todos y no solo del departamento de seguridad informática por que el eslabón más débil de la cadena de seguridad informática es el usuario final.

- Se requiere el apoyo y el compromiso de la alta directiva para el cumplimiento de las normatividad establecida.

- Se debe conocer de las tendencias relacionadas a la seguridad informática e ingeniería social para poder prevenir futuros riesgos.

- Conforme al desarrollo tecnológico se debe establecer controles acorde a la adaptación de la tecnología para poder controlar los incidentes informáticos que se puedan generar.

- Se debe hacer un seguimiento adecuado a las directrices establecidas para garantizar la información.

13. REFERENCIAS

13.1 BIBLIOGRAFÍA

- ACISSI, et al. Seguridad informática - Ethical Hacking: Conocer el ataque para una mejor defensa.2 ed. [s.l.]:2013
- CCN y TB·SECURITY. GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-817): Criterios comunes para la Gestión de Incidentes de Seguridad en el Esquema Nacional de Seguridad (ENS): Editor y Centro Criptológico Nacional, 2012.
- International Organization for Standarization. Information technology - Security techniques - Information security management systems – Requirements. ISO 27001. Edition 2013.

13.2 CIBERGRAFÍA

- 27001Academy. Disponible en: <http://www.iso27001standard.com/es/que-es-iso-27001/>
- PMG-SSI. Disponible en:< http://www.pmg-ssi.com/2014/11/iso-270012015-un-cambio-en-la-integracion-de-los-sistemas-de-gestion/>
- QualityTrends. Disponible en: <http://qualitytrends.squalitas.com/index.php/item/186-principales-cambios-de-la-nueva-version-de-iso-27001>
- The ISO 27000 Directory. Disponible en: <http://www.27000.org/iso-27002.htm>
- TANGIENT LLC. Wikispaces. Disponible en: < http://seguridadinformaticasmr.wikispaces.com/TEMA 1- SEGURIDAD IFORMÁTICA >
- SearhchDataCenter.com/es. Disponible en: <http://searchdatacenter.techtarget.com/es/definicion/Que-es-Plan-de-Recuperacion-de-Desastres-DRP>
- MOLIST, Mercè. Ingeniería Social Mentiras en la Red. Disponible en: <http://ww2.grn.es/merce/2002/is.html>
- SANDOBAL CASTELLANOS, Edgar Jair. Ingeniería Social: Corrompiendo la mente humana .Disponible en: <http://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana#_ftn1>